

En adoptant Progress Flowmon, Volkswagen Slovakia permet à ses équipes IT de bénéficier d'une vue d'ensemble sur son infrastructure

ÉTUDE DE CAS



SECTEUR
Automobile

PRODUIT
Progress® Flowmon®

PAYS
Slovaquie

Le défi

Volkswagen est l'un des plus importants employeurs en Slovaquie, avec près de 11 000 employés répartis sur deux sites de production.

Volkswagen Slovakia dispose d'une vaste infrastructure informatique répartie sur deux sites. Ses départements informatiques et de technologie opérationnelle (OT) exploitent et surveillent 100 000 adresses IP, 8 000 identifiants d'utilisateur et des centaines de machines automatisées. La complexité croissante des réseaux IT et OT a poussé le constructeur automobile à mettre en place de nouvelles stratégies de surveillance et de détection des anomalies en matière de sécurité.

« La politique dite "Zero Trust" est l'une des initiatives les plus significatives que nous ayons mises en œuvre. Actuellement, les périmètres de sécurité classiques n'existent plus, » explique Marian Klaco, Chief Information Security Officer, Volkswagen Slovakia. « Cela s'explique par la complexité croissante liée à l'utilisation de services cloud dans les environnements IT et OT, à l'utilisation de dispositifs IoT et à la complexité accrue des attaques informatiques et de la chaîne d'approvisionnement. »

Volkswagen Slovakia souhaitait se doter d'un outil de sécurité flexible, capable de surveiller l'ensemble de l'entreprise. La complexité de l'infrastructure IT et OT constituant une surface d'attaque plus étendue, l'équipe voulait la surveiller de manière proactive et résoudre les problèmes de manière plus efficace.

Après avoir contacté Progress, réalisé un audit préalable et une démonstration de faisabilité avec Progress® Flowmon®, l'entreprise a choisi de déployer Flowmon à l'échelle de l'entreprise.

La solution

Quelques produits spécifiques de la solution Flowmon sont utilisés par Volkswagen Slovakia. L'équipe informatique utilise le système de détection des anomalies (ADS) de Flowmon pour localiser les anomalies au sein des protocoles de communication réseau. Par exemple, si une communication incohérente passe par des serveurs proxy, le système ADS de Flowmon est déployé pour trouver, examiner et supprimer toute menace. M. Klaco souligne l'utilité de cette fonctionnalité de Flowmon pour protéger, surveiller et sécuriser l'infrastructure de son réseau.

« La politique dite "Zero Trust" est l'une des initiatives les plus significatives que nous ayons mises en œuvre. Actuellement, les périmètres de sécurité classiques n'existent plus. Cela s'explique par la complexité croissante liée à l'utilisation de services cloud dans les environnements IT et OT, à l'utilisation de dispositifs IoT et à la complexité accrue des attaques informatiques et de la chaîne d'approvisionnement. »

Marian Klaco
Chief Information Security
Officer, Volkswagen
Slovakia

« La fonctionnalité ADS (Anomaly Detection System) de Flowmon nous permet d'identifier, d'étudier et d'éliminer les anomalies dans les communications de notre réseau. Elle nous permet d'identifier les comportements malveillants dans l'utilisation de nos systèmes et de nos applications. En raison de la complexité de notre infrastructure, il est nécessaire d'être en mesure d'éliminer les faux positifs dans la surveillance de la sécurité et c'est ce que Flowmon ADS réalise parfaitement. »

Marian Klaco
Chief Information Security Officer, Volkswagen Slovakia

« Les fonctionnalités de Flowmon nous permettent d'identifier, d'étudier et d'éliminer les anomalies dans la communication de notre réseau. Flowmon nous aide à identifier les comportements malveillants dans l'utilisation de nos systèmes et applications, » explique M. Klaco. « En raison de la complexité de notre infrastructure, il est nécessaire d'être en mesure d'éliminer les faux positifs dans la surveillance de la sécurité et c'est ce que Flowmon ADS réalise parfaitement. »

La sonde Flowmon est une autre composante utilisée par les services informatiques pour examiner le trafic provenant des applications, ainsi que pour capturer le trafic réseau à des fins d'analyse. En particulier, M. Klaco et son équipe utilisent Packet Investigator et sa capacité d'analyse automatisée pour examiner plus en détail les problèmes détectés dans le trafic capturé.

Les résultats

Flowmon est désormais largement utilisé par le service informatique du constructeur automobile, qui se compose d'équipes chargées du réseau, des serveurs, de l'assistance aux points d'accès ainsi que des opérations de sécurité. Parmi les autres cas d'utilisation de Flowmon figurent la collecte de données NetFlow, la localisation du trafic provenant des serveurs de gestion de la configuration et la vérification de l'activité des bureaux et des clients. Cela a permis d'améliorer l'efficacité des workflows en localisant et en corrigeant les anomalies de sécurité au sein de l'infrastructure complexe.

« La complexité de nos réseaux informatiques, en particulier des réseaux OT, s'accroît en raison de l'intégration de nouveaux produits dans les lignes de production. Par exemple, avec la maintenance prédictive ou la surveillance conditionnelle dans la production, l'automatisation des processus de production existants, l'intégration des services cloud dans la production, etc, » explique M. Klaco.

« Toutes ces activités augmentent les exigences en matière d'opérations de sécurité afin de préserver la fiabilité de nos infrastructures. »

À propos de Volkswagen Slovakia

Volkswagen Slovakia a été fondée en 1991 et est l'un des plus grands investisseurs étrangers dans le pays. En 30 ans d'existence, plus de 6 500 000 véhicules ont quitté ses ateliers pour des acheteurs du monde entier. L'usine de Bratislava est également la seule usine au monde à produire des véhicules pour quatre marques automobiles différentes. Volkswagen Touareg, Audi Q7, Audi Q8, Porsche Cayenne, Porsche Cayenne Coupé, ŠKODA KAROQ, ainsi que Volkswagen up ! et e-up ! Pour plus d'informations, rendez-vous sur sk.volkswagen.sk/sk



Adoptez Progress® Flowmon® pour améliorer la visibilité de votre propre infrastructure complexe et pour éliminer les menaces de sécurité qui pèsent sur le service informatique de votre entreprise.

À propos de Progress

Dans un monde où la technologie est omniprésente, [Progress](https://www.progress.com) (Nasdaq : PRGS) accompagne les entreprises dans l'accélération de leurs cycles d'innovation et de leur réussite. En tant que fournisseur de confiance des meilleures solutions pour développer, déployer et superviser des applications métiers critiques, Progress permet à ses clients de développer les solutions et les expériences dont ils ont besoin, de les déployer où et comme ils le souhaitent et de les superviser en toute sécurité. Des centaines de milliers d'entreprises, dont 1 700 éditeurs de logiciels et 3,5 millions de développeurs, font confiance à Progress pour atteindre leurs objectifs, en toute sérénité. Pour en savoir plus, rendez-vous sur www.progress.com, et retrouvez-nous sur [LinkedIn](#), [YouTube](#), [Twitter](#), [Facebook](#) et [Instagram](#).

© 2023 Progress Software Corporation et/ou ses filiales ou sociétés affiliées. Tous droits réservés. Rev 2023/07 RITM0193663FR



[f /progresssw](#)
[t /progresssw](#)
[y /progresssw](#)
[in /progress-software](#)
[o /progress_sw_](#)